CrystaX NDK - Bug #1505

Basic hello-world example get crashed on call of getauxval() before libcrystax is initialized

09/13/2016 12:30 PM - Dmitry Moskalchuk

Status:	Open	**Start date:**	09/13/2016
Priority:	Urgent	**Due date:**	
Assignee:	Dmitry Moskalchuk	**% Done:**	0%
Category:	libcrystax	**Estimated time:**	0.00 hour
Target version:	11.0.0		
CPU Architecture:		**Android version:**	
Host OS:		**CrystaX Version:**	11.0.0
Toolchain:			

Description

```
## ADBRUNNER.58296 2016-09-13 09:29:41.484 UTC [04157df46d967829] EXEC: /Users/crystax/work/ndk/samples/cmake/build/hello-world
## ADBRUNNER.58296 2016-09-13 09:29:41.485 UTC [1015fafc27662e05] LOCK  (attempt #1): /Users/crystax/work/ndk/samples/cmake/build/hello-world
## ADBRUNNER.58296 2016-09-13 09:29:41.491 UTC [1015fafc27662e05] START (attempt #1): /Users/crystax/work/ndk/samples/cmake/build/hello-world
## ADBRUNNER.58296 2016-09-13 09:29:41.492 UTC [1015fafc27662e05] RUN:  mkdir -p /data/local/tmp/adbrunner/armeabi-v7a/tmp && mkdir -p /data/local/tmp/adbrunner/armeabi-v7a/lib && mkdir -p /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3 && mkdir -p /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/bin && mkdir -p /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/data
## ADBRUNNER.58296 2016-09-13 09:29:41.661 UTC [1015fafc27662e05] COPY: /Users/crystax/work/ndk/samples/cmake/build/hello-world -> /Users/crystax/.crystax/adbrunner/stripped/armeabi-v7a/hello-world.f12d7e54fc3277b2acb0dfeaa2ac5bf133059b95a78219f5caada141bee9197c
## ADBRUNNER.58296 2016-09-13 09:29:41.661 UTC [1015fafc27662e05] STRIP: /Users/crystax/.crystax/adbrunner/stripped/armeabi-v7a/hello-world.f12d7e54fc3277b2acb0dfeaa2ac5bf133059b95a78219f5caada141bee9197c
## ADBRUNNER.58296 2016-09-13 09:29:41.667 UTC [1015fafc27662e05] PUSH: /Users/crystax/.crystax/adbrunner/stripped/armeabi-v7a/hello-world.f12d7e54fc3277b2acb0dfeaa2ac5bf133059b95a78219f5caada141bee9197c -> /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/bin/exeb4f45cc609a04a82aec445098b859dfb
## ADBRUNNER.58296 2016-09-13 09:29:41.685 UTC [1015fafc27662e05] [100%] /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/bin/exeb4f45cc609a04a82aec445098b859dfb
## ADBRUNNER.58296 2016-09-13 09:29:41.685 UTC [1015fafc27662e05] RUN:  chmod 0755 /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/bin/exeb4f45cc609a04a82aec445098b859dfb
## ADBRUNNER.58296 2016-09-13 09:29:41.770 UTC [1015fafc27662e05] RUN:  grep -q -x 285d691337ef9a5518f72c306438c0cb1d37eb0913b8ae24cfec018146689968 /data/local/tmp/adbrunner/armeabi-v7a/lib/libcrystax.so.sha256 2>/dev/null
## ADBRUNNER.58296 2016-09-13 09:29:41.845 UTC [1015fafc27662e05] RUN:  grep -q -x ed590847aebd95d928ca610f39799e854d0ece4683520e61636bcdc6efb1ea3e /data/local/tmp/adbrunner/armeabi-v7a/lib/libgnustl_shared.so.sha256 2>/dev/null
## ADBRUNNER.58296 2016-09-13 09:29:41.908 UTC [1015fafc27662e05] RUN:  log LOGCAT-TAG-38f496512cec401dbc727fc350c2d7d1 && cd /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/data && LD_LIBRARY_PATH=/data/local/tmp/adbrunner/armeabi-v7a/lib TMPDIR=/data/local/tmp/adbrunner/armeabi-v7a/tmp /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/bin/exeb4f45cc609a04a82aec445098b859dfb
## ADBRUNNER.58296 2016-09-13 09:29:42.120 UTC [1015fafc27662e05]    > Segmentation fault
## ADBRUNNER.58296 2016-09-13 09:29:42.120 UTC [1015fafc27662e05] RUN [$?=139]: log LOGCAT-TAG-38f496512cec401dbc727fc350c2d7d1 && cd /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/data && LD_LIBRARY_PATH=/data/local/tmp/adbrunner/armeabi-v7a/lib TMPDIR=/data/local/tmp/adbrunner/armeabi-v7a/tmp /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/bin/exeb4f45cc609a04a82aec445098b859dfb
## ADBRUNNER.58296 2016-09-13 09:29:42.121 UTC [1015fafc27662e05]    *
## ADBRUNNER.58296 2016-09-13 09:29:42.121 UTC [1015fafc27662e05]    *
## ADBRUNNER.58296 2016-09-13 09:29:42.121 UTC [1015fafc27662e05]    * === BEGIN OF ENVIRONMENT ===
```

```
## ADBRUNNER.58296 2016-09-13 09:29:42.121 UTC [1015fafc27662e05]    * CMD: /Users/crystax/work/ndk/samples/cmake/build/hello-world
## ADBRUNNER.58296 2016-09-13 09:29:42.121 UTC [1015fafc27662e05]    * PWD: /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/bin
## ADBRUNNER.58296 2016-09-13 09:29:42.121 UTC [1015fafc27662e05]    * NDK: /opt/android/crystax-ndk-10.3.2-b903 - CrystaX NDK v10.3.2 (64-bit)
## ADBRUNNER.58296 2016-09-13 09:29:42.121 UTC [1015fafc27662e05]    * === END OF ENVIRONMENT ===
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    *
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    * === BEGIN OF LOGCAT ===
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    * 09-13 12:31:35.943 28296 28296 F libc    : Fatal signal 11 (SIGSEGV), code 1, fault addr 0x0 in tid 28296 (exeb4f45cc609a0)
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   : Build fingerprint: 'samsung/zenltexx/zenlte:6.0.1/MMB29K/G928FXXS2BPH1:user/release-keys'
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   : Revision: '9'
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   : ABI: 'arm'
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   : pid: 28296, tid: 28296, name: exeb4f45cc609a0  >>> /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3/bin/exeb4f45cc609a04a82aec445098b859dfb <<<
## ADBRUNNER.58296 2016-09-13 09:29:42.488 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 E DEBUG   : AM write failed: Broken pipe
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x0
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   :     r0 00000019  r1 f6f6eec8  r2 00000000  r3 f70f2804
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   :     r4 f6f6a594  r5 f7292a48  r6 f724e9c4  r7 00000001
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   :     r8 f729270c  r9 0000000b  sl f724e9c4  fp f728b324
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6708  6708 F DEBUG   :     ip f6f6a630  sp ff9124d8  lr f6f0eddf  pc f70a2c80  cpsr 000e0030
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.003  6907 14820 W NativeCrashListener: Couldn't find ProcessRecord for pid 28296
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   : backtrace:
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #00 pc 00092c80  /data/local/tmp/adbrunner/armeabi-v7a/lib/libcrystax.so (getauxval+7)
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #01 pc 0001addb  /system/lib/libc.so (_Z18__libc_init_commonR19KernelArgumentBlock+62)
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #02 pc 00016735  /system/lib/libc.so (exit+16)
## ADBRUNNER.58296 2016-09-13 09:29:42.489 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #03 pc 00016745  /system/lib/libc.so (_ZL14__libc_preinitv+12)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #04 pc 00002385  /system/bin/linker (__dl__ZN6soinfo13call_functionEPKcPFvvE+48)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #05 pc 0000244f  /system/bin/linker (__dl__ZN6soinfo10call_arrayEPKcPPFvvEjb+134)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #06 pc 00002615  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+160)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #07 pc 000025c9  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+84)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #08 pc 000025c9  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+84)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #09 pc 000025c9  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+84)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6708 F DEBUG   :     #10 pc 000025c9  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+84)
```

```
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6
708 F DEBUG   :     #11 pc 0000645f  /system/bin/linker (__dl___linker_init+1278)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.023  6708  6
708 F DEBUG   :     #12 pc 00001538  /system/bin/linker (_start+4)
## ADBRUNNER.58296 2016-09-13 09:29:42.490 UTC [1015fafc27662e05]    * 09-13 12:31:36.053  6708  6
708 F DEBUG   :
## ADBRUNNER.58296 2016-09-13 09:29:42.491 UTC [1015fafc27662e05]    * 09-13 12:31:36.053  6708  6
708 F DEBUG   : Tombstone written to: /data/tombstones/tombstone_05
## ADBRUNNER.58296 2016-09-13 09:29:42.491 UTC [1015fafc27662e05]    * 09-13 12:31:36.053  6708  6
708 E         : ro.product_ship = true
## ADBRUNNER.58296 2016-09-13 09:29:42.491 UTC [1015fafc27662e05]    * 09-13 12:31:36.053  6708  6
708 E         : ro.debug_level = 0x4f4c
## ADBRUNNER.58296 2016-09-13 09:29:42.491 UTC [1015fafc27662e05]    * 09-13 12:31:36.053  6708  6
708 E         : sys.mobilecare.preload = false
## ADBRUNNER.58296 2016-09-13 09:29:42.491 UTC [1015fafc27662e05]    * 09-13 12:31:36.053 16051 16
051 E audit   : type=1701 msg=audit(1473759096.053:7709): auid=4294967295 uid=2000 gid=2000 ses=42
94967295 subj=u:r:shell:s0 pid=28296 comm="exeb4f45cc609a0" reason="memory violation" sig=11
## ADBRUNNER.58296 2016-09-13 09:29:42.491 UTC [1015fafc27662e05]    * === END OF LOGCAT ===
## ADBRUNNER.58296 2016-09-13 09:29:42.551 UTC [1015fafc27662e05]    *
## ADBRUNNER.58296 2016-09-13 09:29:42.551 UTC [1015fafc27662e05]    * === BEGIN OF NDK-STACK ===
## ADBRUNNER.58296 2016-09-13 09:29:42.562 UTC [1015fafc27662e05]    * ********** Crash dump: ****
******
## ADBRUNNER.58296 2016-09-13 09:29:42.562 UTC [1015fafc27662e05]    * Build fingerprint: 'samsung
/zenltexx/zenlte:6.0.1/MMB29K/G928FXXS2BPH1:user/release-keys'
## ADBRUNNER.58296 2016-09-13 09:29:42.563 UTC [1015fafc27662e05]    * pid: 28296, tid: 28296, nam
e: exeb4f45cc609a0  >>> /data/local/tmp/adbrunner/armeabi-v7a/35de6cf5-551e-499e-be67-96fbe5aa9de3
/bin/exeb4f45cc609a04a82aec445098b859dfb <<<
## ADBRUNNER.58296 2016-09-13 09:29:42.563 UTC [1015fafc27662e05]    * signal 11 (SIGSEGV), code 1
 (SEGV_MAPERR), fault addr 0x0
## ADBRUNNER.58296 2016-09-13 09:29:42.563 UTC [1015fafc27662e05]    * Stack frame #00 pc 00092c80
  /data/local/tmp/adbrunner/armeabi-v7a/lib/libcrystax.so (getauxval+7): Routine getauxval at /Vol
umes/HD2/cislave/workspace/ndk-build-all/HOST/darwin/LABEL/ndk-build/platform/ndk/sources/crystax/
gen/bionic/libc/bionic/mangled-getauxval.cpp:39 (discriminator 1)
## ADBRUNNER.58296 2016-09-13 09:29:42.564 UTC [1015fafc27662e05]    * Stack frame #01 pc 0001addb
  /system/lib/libc.so (_Z18__libc_init_commonR19KernelArgumentBlock+62)
## ADBRUNNER.58296 2016-09-13 09:29:42.564 UTC [1015fafc27662e05]    * Stack frame #02 pc 00016735
  /system/lib/libc.so (exit+16)
## ADBRUNNER.58296 2016-09-13 09:29:42.564 UTC [1015fafc27662e05]    * Stack frame #03 pc 00016745
  /system/lib/libc.so (_ZL14__libc_preinitv+12)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #04 pc 00002385
  /system/bin/linker (__dl__ZN6soinfo13call_functionEPKcPFvvE+48)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #05 pc 0000244f
  /system/bin/linker (__dl__ZN6soinfo10call_arrayEPKcPPFvvEjb+134)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #06 pc 00002615
  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+160)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #07 pc 000025c9
  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+84)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #08 pc 000025c9
  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+84)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #09 pc 000025c9
  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+84)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #10 pc 000025c9
  /system/bin/linker (__dl__ZN6soinfo17call_constructorsEv+84)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #11 pc 0000645f
  /system/bin/linker (__dl___linker_init+1278)
## ADBRUNNER.58296 2016-09-13 09:29:42.565 UTC [1015fafc27662e05]    * Stack frame #12 pc 00001538
  /system/bin/linker (_start+4)
## ADBRUNNER.58296 2016-09-13 09:29:42.566 UTC [1015fafc27662e05]    * === END OF NDK-STACK ===
## ADBRUNNER.58296 2016-09-13 09:29:42.647 UTC [1015fafc27662e05] EXIT: 139 (took 0:00:01 on 'SM-G
928F')
```